April 2023 | **Volume 12** | Issue 4

Curry Insurance Agency

NON-DISPARAGEMENT, CONFIDENTIALITY CLAUSES

NLRB Deals Blow to Severance Agreements

THE NATIONAL Labor Relations Board has issued a decision that non-disparagement and confidentiality clauses in employee severance agreements are illegal.

The board ruled that these provisions stifle employees' and ex-employees' rights under Title 7 of the National Labor Relations Act to discuss work and their employer with one another, among other things.

Since the NLRB's decision applies to both unionized and non-unionized workers, legal experts advise all employers to revisit their severance agreement templates. However, the decision only covers employees – and not severance agreements for supervisors or managers, who are not afforded rights under Title 7.

Decision is far-reaching

In the case before the NLRB, an employer decided to lay off a group of union workers and offered them a severance agreement that included them receiving additional months of pay and benefits depending on their tenure with the company.

It also included a standard confidentiality clause and non-dispargement clause that are found in many severance agreements:

> ***Confidentiality Agreement.*** *"The Employee acknowledges that the terms of this Agreement are confidential and agrees not to disclose them to any third person, other than spouse, or as necessary to professional advisors for the purposes of obtaining legal counsel or tax advice, or unless legally compelled to do so by a court or administrative agency of competent jurisdiction."*

> ***Non-Disparagement Agreement.*** *"At all times hereafter, the Employee agrees not to make statements to Employer's employees or to the general public which could disparage or harm the image of Employer, its parent and affiliated entities and their officers, directors, employees, agents and representatives."*

The ruling

The board ruled that merely including non-disparagement and non-disclosure agreements in severance agreements constituted unfair labor practices under Title 7, which guarantees employees (in part):

"The right to self-organization ... and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection."

Translation: Workers have the right to discuss their jobs and even complain about their employer and management to one another.

The takeaway

The ruling may be appealed, but for now it stands and is not on hold.

The decision will affect employers in virtually every industry and regardless of whether they have union workers or not.

If you plan to continue using severance agreements going forward, you should consult your legal counsel, particularly if your current agreements contain the clauses that offended the NLRB. ❖

CONTACT US

Curry Insurance Agency

If you have any questions regarding any of these articles or have a coverage question, please call us at:

ISU Curry Insurance Agency
489 E. Colorado Boulevard
Pasadena, CA 91101
Phone: 626-449-3870
Fax: 626 449-5268
License No. : 0588757

CYBER RISKS

Phishing Attacks on Business Smartphones Grow

PHISHING ATTACKS on enterprise and employees' smartphones continue plaguing businesses, with attacks increasing 10% in 2022 from 2021, according to a new report.

As more businesses have adopted bring-your-own-device (BYOD) policies, the risks grow for these attacks, which can be costly.

Last year, 11.8% of mobile enterprise users clicked on six or more malicious links, compared with just 1.6% in 2020, which "indicates users are having a tougher time recognizing phishing attempts," according to the report by cyber security firm Lookout Inc.

What is phishing?

Phishing attacks try to coax a target to reveal personal information like passwords or credentials in an e-mail that looks like it's been sent from a reputable source.

Messages are often enticing or convey a sense of urgency.

Typical Phishing Topics

- Prize notifications
- Tech support notifications
- Shipping notifications
- Contact-tracing messages that request personal information.

The dangers

Successful phishing attacks can have costly implications for a business, including:

Rerouting payments – Attackers gain access to your accounts so they can reroute legitimate vendor payments to their own accounts by modifying invoices. They may also gain access to an employee's e-mail and impersonate them, modify content of e-mails and request funds.

System outage – If the phishing attack is a ransomware attack, it can shut down your entire database and website. Depending on how much you rely on your systems, the damage could be a few hundred dollars or tens of thousands in lost revenue.

Data theft – A phishing attack can also result in sensitive company data being compromised or stolen. If personal data is exposed, it could have regulatory consequences, including fines.

What you can do

There are steps you can take to protect your organization, its company-owned and BYOD devices from phishing attacks. Cyber security firm TechTarget recommends:

Using mobile security tools – Security solutions called endpoint management tools may add a layer of protection to mobile devices. These include:

- Symantec Endpoint Protection Mobile
- Trend Micro Mobile Security
- Kaspersky Endpoint Security
- Microsoft Intune
- F-Secure Mobile Security.

Other solutions that can filter out spam text messages and block known sources of phishing attacks include:

- RoboKiller
- Apple iPhone built-in spam filters
- SpamHound SMS Spam Filter.

Creating mobile device policies – Establish smartphone policies for your employees to follow. If you have an IT person, they can set up these policies through mobile device management tools like Microsoft Intune or MobileIron.

These tools can keep employees from responding to messages from unknown sources or clicking on links send via text messages. They can also block messages from unknown sources.

Training your employees – Train your employees to not click on links in messages from unknown sources and to be wary if a co-worker is asking them to click on a link.

Provide examples of how to identify phishing attacks, what actions to take if they receive a request for information, and how to check that the mail is from a trusted source. ❖

NEW GUIDANCE

FMLA Leave Can Be Taken in Hourly Increments

THE U.S. Department of Labor recently issued new guidance on the federal Family Medical Leave Act that has upended the notion of what qualifies as leave under the statute.

Its Wage and Hour Division in February issued a guidance letter noting that employees with a serious illness may use intermittent leave under the FMLA to work a reduced schedule for "an indefinite period." That is a significant departure from the typical FMLA scenario where workers will take days, weeks or months off from work for a qualifying reason under the law.

The ruling paves the way for workers with serious health conditions that may limit how many hours they can work in a day to do reduced hours, which will count towards the law's leave limit of 12 working weeks per 12-month period.

In other words, if an FMLA-eligible employee reduced their working hours by two every day, they would never exhaust their allowed leave (two hours a day for an entire year).

The FMLA entitles eligible employees to take unpaid job-protected leave for qualifying family and medical reasons with continuation of group health insurance coverage.

The case and opinion

The company that sought the opinion clarifying the law required its employees to regularly work 10-hour shifts to meet its 24-hour operational needs. Several of its workers asked the company under the FMLA to limit their shifts to eight hours.

It asked the Wage and Hour Division to render an opinion if that would be an appropriate use of the law.

Here is the ground-breaking interpretation of the law in the opinion that followed:

"In this case, if an employee would normally be required to work more than eight hours a day but is unable to do so because of an FMLA-qualifying reason, the employee may use FMLA leave for the remainder of each shift, and the hours which the employee would have otherwise been required to work are counted against the employee's FMLA leave entitlement."

The Wage and Hour Division added that employees can continue to use FMLA leave until they exhaust their leave, but if an employee only takes a few hours off every day from a workday that's longer than eight hours, they could theoretically never exhaust their leave and be able to reduce their hours indefinitely.

The takeaway

This guidance changes the dynamic of family medical leave for both employers and employees.

In one sense, if employees are FMLA-eligible but still feel they can work a restricted amount of hours, it could be a benefit for an employer that needs the manpower they may lose with someone who takes weeks off work.

It would also allow the employee to earn a paycheck (albeit reduced by the hours they don't work).

But for employers that need all hands on deck and working full shifts, this could be a burden.

If you are faced with a situation where an employee requests a restricted work schedule under the auspices of the FMLA, discuss your plans with legal counsel.❖

DRIVER SAFETY

Tapping Technology to Tackle Distracted Driving

MORE COMPANIES with fleets and commercial drivers are turning to technology to prevent their workers from using their phones while driving. And lately, insurers have started partnering with tech companies to offer these technologies to their commercial auto clients.

Using a hand-held mobile phone while driving a commercial vehicle can result in U.S. Department of Transportation fines of up to $2,750 for drivers, and $11,000 for employers who allow or require drivers to use a hand-held communications device while behind the wheel.

But the consequences are more than financial as lives and property are on the line.

Tech and fleets

It's estimated that phone-related accidents cost commercial fleet operators over $2 billion per year, despite the fact that virtually every state has laws on its books banning use of hand-held phones and interacting with smartphones.

That's why trucking businesses and companies with fleets of vehicles are increasingly incorporating new technologies coupled with stringent safety regimens.

Driver cameras – Among more effective technologies are driver cameras that can monitor distracted movements indicating the use of a phone or other device. These cameras monitor facial and eye movements, and if showing signs of distraction, prompt an alert or warning. This would also work to detect fatigue, drowsiness and/or sleep apnea.

Apps that disable other apps – Employers can also install apps on their drivers' smartphones that disable various functions and apps on their phones when the vehicle is in motion.

Once such app is NoCell, which operates in the background and allows employers to disable disruptive apps and cell phone functions while drivers are on the road. The employer can choose which apps NoCell should disrupt when the vehicle is in motion and/or not in Park.

Nationwide Insurance Co. recently contracted with NoCell, which it plans to provide to its commercial vehicle insurance customers.

Another app, Live Undistracted's PhoneSafe technology, disables phone functions and apps while the vehicle is out of Park.

When installed on the driver's phone, it detects when the vehicle is taken out of Park, triggering its safe mode. Managers receive real-time alerts for phone policy violations.

Insurers in on the act too

Some insurers have gotten into the game themselves by creating their own technology.

New Jersey-based Selective Insurance Co. created Selective Drive, a fleet management tool that includes monitoring of drivers, including phone usage.

This tool is not an app and can't disable phone functions. But it does give the employer access to driver information, such as real-time speed and time-of-day monitoring, phone usage, and sudden acceleration and braking activity, which may identify risky behavior with their drivers before it becomes a problem.

It also includes real-time vehicle tracking, vehicle health and monitoring, and geo-tracking, which alerts drivers when they deviate from routes or driving boundaries.

The takeaway

Even the best distracted-driving policy is words on paper, and smartphones offer such temptations that fleet drivers regularly break the rules.

It makes sense to use technology to further constrain your drivers' ability to use their phone when they are driving on the job. There are a number of technologies that employers can use besides the ones mentioned above.

It pays to look into it. It may save someone's life and it may prevent a massive headache and legal troubles for your organization. ❖